A simple protocol for secure decoy-state quantum key distribution with a loosely controlled source

Xiang-Bin Wang[1,*] and Cheng-Zhi Peng[1,†]

[1]*Department of Physics, Tsinghua University, Beijing 100084, China*

Abstract

We show that decoy-state quantum key distribution is unconditionally secure even there are errors in the intensity control provided that the upper-bound of intensity of all pulses are known. In our protocol, we simply let Alice each time first produce a father pulse and then determine to produce intensity μ or μ' by attenuation. In calculating the fraction of single-photon counts, Alice only need assume that she had used intensities of $\tilde{\mu}, \tilde{\mu}'$ exactly even though there are fluctuations in the actual intensity control.

PACS numbers: 03.67.Dd, 42.81.Gs, 03.67.Hk

Recently, some methods[1, 2, 3, 4, 5, 6, 7, 8] have been proposed for secure quantum key distribution (QKD)[9, 10, 11] with coherent states[12, 13, 14]. One of these methods is the so called decoy-state method[1, 2, 3, 4, 5] where Alice randomly changes the intensity of her pulses among a few values and then she can verify the fraction of tagged bits (those counts at Bob's side due to multi-photon pulses from Alice) or un-tagged bits (single-photon counts) in the raw key. A secure final key can be distilled by using the separate theoretical results[15] if one knows the upper bound of the fraction of tagged bits or equivalently, the lower bound of the fraction of un-tagged bits. The goal of decoy-state method is to verify such bounds faithfully and efficiently.

So far a number of experiments on decoy-state QKD have been done[16, 17, 18], in optical fiber or in free space, in polarization space or with phase-coding. However, the existing theory of decoy-state method assumes the exact control of pulse intensities. A new problem arose in practice is how to carry out the decoy-state method efficiently given the inexact control of pulse intensity. As we have shown[19], actually, one can verify the single-photon counts rather efficiently with simple tomography even though the intensity fluctuations of each light pulses are large. However, there Alice needs additional operation of tomography. Also, to guarantee the randomness of intensity fluctuation, Alice needs to do something more, e.g., take a feedback control of attenuation. Here we present a simpler protocol for decoy-state method QKD. This protocol assumes a set-up identical with that of the existing experiment, but one needs the information of intensity upper-bound of all pulses.

We consider the 3-intensity decoy-state method[2] where Alice is supposed to choose an intensity out of $\{0, \mu, \mu'\}$ randomly for each pulses. But in a real set-up, she cannot control the intensity exactly for each pulse as she wants to. As we have shown already[19], a bit inexact control in vacuum doesn't matter. Therefore here we shall only consider the effects of inexact control of μ, μ'.

For clarity, lets first consider an *ideal protocol* with exact intensity control, as shown in Fig. 1:a). At any time t, if Alice wants to send a pulse of intensity μ or μ', she first produces a father pulse of intensity Ω. After that she attenuates by the pulse $A(t) = \mu/\Omega$ or $A(t) = \mu'/\Omega$ randomly and a pulse of intensity μ or μ' is produced randomly and sent out to Bob. In this ideal protocol, Both Ω and $A(t)$ are controlled exactly.

In practice, we use a similar protocol as shown in Fig. 1:b). Alice *wants* to produce an intensity Ω for the father pulse. She then takes the same random attenuations as that in the

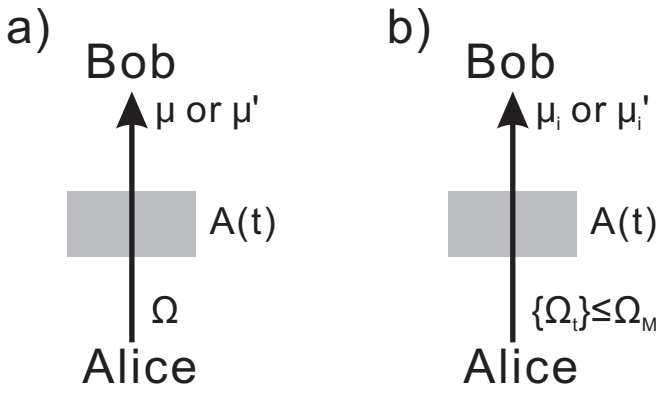

FIG. 1: a) The ideal protocol that Alice can produce constant intensity Ω for the father pulse therefore intensity μ, μ' are controlled exactly. b) The true protocol used in practice. At each time, Alice *wants* to produce intensity Ω for the father pulse, however, she actually produces $\{\Omega_t\}$ at each time t. Consequently, the intensities of output pulses are $\{\mu_i\}, \{\mu_i'\}$. We assume that Alice can control the attenuator $A(t)$ exactly in a real protocol. After a father pulse is produced, Alice randomly choose the attenuation factor by $A(t) = \mu/\Omega$ or $A(t) = \mu'/\Omega$. Here the subscript t is from 1 to $N + N'$, subscript i for $\{\mu_i\}$ is from 1 to N, subscript i for $\{\mu_i'\}$ is from 1 to N'.

ideal protocol. Here we assume that Alice can control the attenuation factors of $A(t)$ exactly (either μ/Ω or μ'/Ω) but she can not control Ω exactly. (There are many ways to control the attenuator $A(t)$ exactly. For example, we can use unbalanced beam-splitters.) In each time, she has actually produced intensities of $\{\Omega_t\}$ for the father pulses. (Here t is a discrete number.)Although we can never control the intensity exactly, by our currently existing technology, we can definitely control the intensity in a small range, say, e.g., controlling the fluctuation between $\pm 20\%$ of Ω. That is to say, Alice knows the upper-bound of $\{\Omega_t\}$. We denote such an upper bound value as Ω_M.

Given this upper-bound value Ω_M, the set-up in Fig. 1:b) is equivalent to a virtual set-up as shown in Fig. 2:a). In the virtual protocol shown in Fig. 2:a), every time a father pulse of constant intensity Ω_M is first produced and then the pulse is attenuated randomly, with attenuation factors of $A'(t) = \frac{\Omega_t}{\Omega_M}$. Alice cannot control this $A'(t)$. After this attenuation, a pulse of intensity Ω_t is produced. Note that $A'(t)$ is independent of μ, μ', since we can imagine that Alice decides to use μ or μ' *after* the attenuation $A'(t)$. Since all attenuators are inside Alice's Lab., it makes no difference if Alice exchange the order of attenuators $A(t)$ and $A'(t)$. The physical meaning of order exchange is that Alice first decides to use μ or μ'

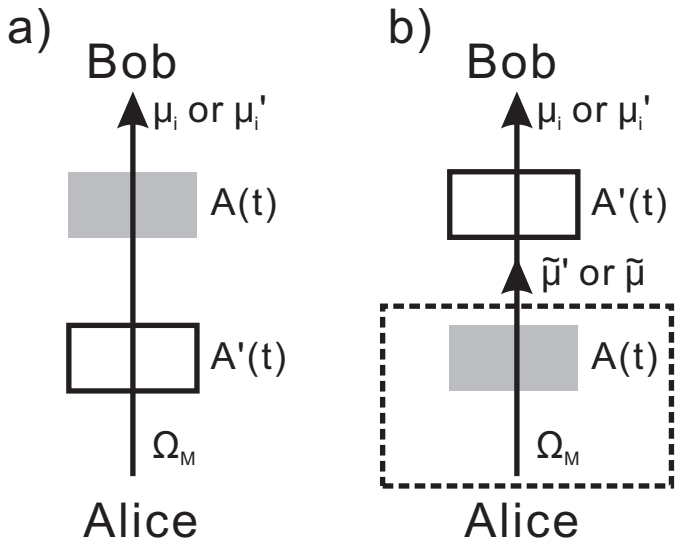

FIG. 2: Equivalent virtual protocols. Our real protocol in Fig. 1:b) is equivalent to a virtual protocol as shown in part a) of this figure. Here Alice first produces a constant intensity Ω_M for each father pulses and then attenuates each of them by attenuator $A'(t)$. After $A'(t)$, the pulse intensity is Ω_t. It makes no difference to the output light if we exchange the order of $A(t)$ and $A'(t)$, therefore a) is equivalent to b). In part b), we can regard the dashed square as our source and $A'(t)$ as part of the channel, if Alice let Eve controls $A'(t)$. In this way, it is equivalent to a decoy-state protocol where Alice has used exact intensities of $\{0, \tilde{\mu}, \tilde{\mu}'\}$.

and then arrange the attenuation $A'(t)$ which is independent of Alice's decision of using μ or μ'. This is just the virtual protocol in Fig. 2:b). In Fig. 2:b), after the pulse passes $A(t)$ but before passes $A'(t)$, the intensity should be either $\tilde{\mu} = \frac{\mu}{\Omega}\Omega_M$ or $\tilde{\mu}' = \frac{\mu'}{\Omega}\Omega_M$ *exactly*. That is to say, during the virtual stage between $A(t)$ and $A'(t)$, the light intensities of each pulses are either exactly $\tilde{\mu}$ or exactly $\tilde{\mu}'$. But after a pulse passes through $A'(t)$, the intensity is changed to inexact values of μ_i or μ_i'. For the security proof of the real set-up in Fig. 1:b), we show the following lemma first.

Lemma: The set-up in Fig. 2:b) is unconditionally secure if Alice regards it as a 3-intensity decoy-state protocol with each light intensities being randomly chosen from $\{0, \tilde{\mu}, \tilde{\mu}'\}$.

Proof: First we suppose Eve controls $A'(t)$. The dashed square can be regarded as an exact source for a decoy-state protocol using intensities $0, \tilde{\mu}, \tilde{\mu}'$. As it has been known already, decoy-state method with exact intensity control is secure given whatever channel. Here what

Eve can do is first using $A'(t)$ for attenuation and then do whatever. This is a only type of specific channel therefore cannot be used to cheat Alice and Bob. In the set-up of Fig. 2:b), actually the attenuator $A'(t)$ is not controlled by Eve, definitely the set-up is secure because Eve cannot attack the protocol better with her power being reduced. In Eve's eyes, $A'(t)$ *could* have been controlled by Alice since it makes no difference to Eve on whether Alice knows the explicit values of $A'(t)$.

Given this lemma, we immediately have the **theorem:** *The set-up shown in Fig. 1:b) is also unconditionally secure if Alice knows that values of* $\{\Omega_t\}$ *are upper-bounded by* Ω_M *and she then does the calculation of fraction of single-photon counts as if she had used a 3-intensity decoy-state protocol with exact intensities of* $\{0, \tilde{\mu}, \tilde{\mu}'\}$. The proof is simply that the final light pulses produced in Fig. 1:b) and final light pulses produced in Fig. 2:b) are identical.

Having this theorem, we now evaluate the efficiency of our protocol. Lets restate our protocol before evaluation. Alice wants to use intensities of $0, \mu = 0.2, \mu' = 0.6$. Every time she sends out nothing to Bob if she chooses to sends out vacuum, otherwise she first produces a father pulse and she *tries* to control the intensities of the father pulse to be constant, say Ω. She then uses exact attenuation of either $0.2/\Omega$ or $0.6/\Omega$. Although she *tries* to produce intensity μ or μ' precisely, there are intensity fluctuations. She knows that ever time the intensity of the father pulse is at most $\lambda\Omega$ ($\lambda \geq 1$). According to our theorem, she needs to calculate the fraction of single-photon counts as if she had just done a decoy-state protocol with intensities of $0, \tilde{\mu} = \lambda\mu, \tilde{\mu}' = \lambda\mu'$.

We consider the normal case where there is no Eve. and a linear channel that has a transmittance η. Normally, Alice and Bob can find the values of $\eta\mu$, $\eta\mu'$ for the counting rates of pulses of supposed intensities of μ, μ', respectively, if there is no dark count. But in calculating the fraction of single-photon counts, Alice has to assume $\tilde{\mu}, \tilde{\mu}'$ as intensities she has used in the protocol. Suppose there are N, N' pulses for the supposed intensities μ, μ' ($N' > N$), respectively. We have the following joint equations[2]:

$$\begin{aligned} & e^{-\lambda\mu} s_0 + \lambda\mu e^{-\lambda\mu} s_1 + c s_c = S; \\ & e^{-\lambda\mu'} s'_0 + \lambda\mu' e^{-\lambda\mu'} s'_1 + \left(\frac{\lambda\mu'}{\lambda\mu}\right)^2 e^{\lambda\mu - \lambda\mu'} s'_c \leq S' \end{aligned} \tag{1}$$

Here $c = 1 - e^{-\lambda\mu} - \lambda\mu e^{-\lambda\mu}$, S and S' are the observed counting rates of pulses of supposed intensity μ, μ', respectively. Parameters of s_x are counting rates for states $|x\rangle\langle x|$ from μ

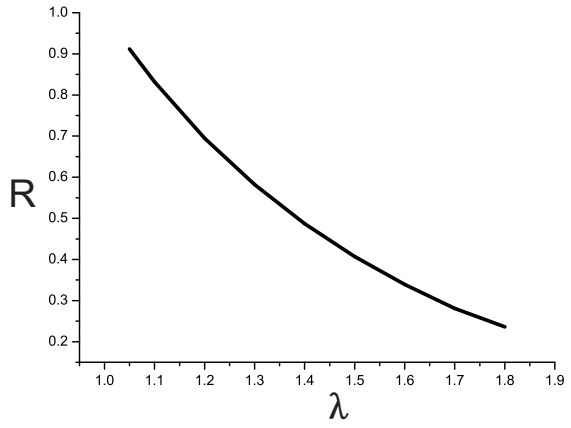

FIG. 3: Comparison of the verified fraction of single photon counting rates between our protocol and an ideal protocol with exact intensity control. Horizontal axis is for the λ value and vertical axis is for the calculated ratio of $R = \frac{\tilde{\Delta}'}{\Delta'}$

pulses ($x = 0, 1$), s_c is the counting rates of state ρ_c (state of those multi-photon pulses) from μ pulses. Parameters s'_x are counting rates of the same state as defined for s_x, but they are for those states from μ' pulses only. The values of s_0, s'_0 can be deduced from the counting rate of those vacuum pulses. Asymptotically, $s_x = s'_x$. Given finite number of pulses, s_x and s'_x can be a bit different. We have

$$\begin{aligned} s'_1 &\geq (1 - r_1)s_1, \ r_1 = 10\sqrt{\tfrac{1}{s_1 \lambda\mu e^{-\lambda\mu}}}; \\ s'_c &\geq (1 - r_c)s_c, \ r_c = 10\sqrt{\tfrac{1}{s_c \lambda^2\mu^2 e^{-\lambda\mu}}}. \end{aligned} \tag{2}$$

Putting this into eqs.(1) we have

$$\begin{aligned} &e^{-\lambda\mu}s_0 + \lambda\mu e^{-\lambda\mu}s_1 + cs_c = S \\ &e^{-\lambda\mu'}s'_0 + \lambda\mu' e^{-\lambda\mu'}(1 - r_1)s_1 + \left(\tfrac{\lambda\mu}{\lambda\mu'}\right)^2 e^{\lambda\mu - \lambda\mu'}(1 - r_c)s_c \leq S'. \end{aligned} \tag{3}$$

Solving the above equations numerically we can obtain the value of s_1. If Alice controls the light intensity exactly, then $\lambda = 1$ in eqs.(3). In a real protocol, Alice cannot control the light intensity exactly therefore $\lambda > 1$. In the calculation, we set $s_0 = s'_0 = 0$, $\eta = 10^{-4}$, $\mu = 0.2$, $\mu' = 0.6$, $S = \eta\mu$, $S' = \eta\mu'$ and $N = 10^9$ We have calculated the values given different λ. And we then compare the fraction of single-photon counts ($\tilde{\Delta}'$) of μ' pulses from a real protocol ($\lambda > 1$) and that(Δ') from the ideal protocol ($\lambda = 1$) by formula

$$R = \frac{\tilde{\Delta}'}{\Delta'} = \frac{\lambda e^{-\lambda\mu'}(1 - r_1)s_1(\lambda)/(\eta\mu')}{e^{-\mu'}(1 - r_1)s_1/(\eta\mu')} = \frac{\lambda e^{-\lambda\mu'}s_1(\lambda)}{e^{-\mu'}s_1} \tag{4}$$

where $s_1(\lambda), s_1$ are the solution of single-photon counting rates with parameter $\lambda > 1$, $\lambda = 1$ in eqs.(3). We have taken a few different λ values in the calculation. Results are shown in Fig. 3.

Acknowledgement. We thank Dr Dong Yang, Jun Zhang and Xian-Min Jin for many helps.

---

* Electronic address: xbwang@mail.tsinghua.edu.cn

† Electronic address: pcz@mail.tsinghua.edu.cn

[1] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[2] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[3] X.-B. Wang, Phys. Rev. A **72**, 012322 (2005).

[4] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. Ma *et al.*, Phys. Rev. A **72**, 012326 (2005).

[5] J.W. Harrington *et al.*, quant-ph/0503002.

[6] R. Ursin et al, quant-ph/0607182.

[7] V. Scarani, A. Acin, G. Robordy, N. Gisin, Phys. Rev. Lett. 92, 057901 (2004); C. Branciard, N. Gisin, B. Kraus, V. Scarani, Phys. Rev. A 72, 032301 (2005).

[8] M. Koashi, Phys. Rev. Lett., 93, 120501(2004); K. Tamaki, N. Lükenhaus, M. Loashi, J. Batuwantudawe, quant-ph/0608082

[9] C.H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conf. on Computers, Systems, and Signal Processing (IEEE, New York, 1984)*, pp. 175-179.

[10] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[11] M. Dusek, N. Lütkenhaus, M. Hendrych, "Quantum Cryptography", in *Progress in Optics VVVX*, edited by E. Wolf (Elsevier, 2006).

[12] M. Bourennane *et al.*, F. Gibson, A. Karlsson, A. Hening, P.Jonsson, T. Tsegaye, D. Ljunggren, and E. Sundberg, Opt. Express **4**, 383 (1999); D. Stucki *et al.*, D. Stucki, N. Gisin, O. Guinnard, G. Ribordy and H. Zbinden, New. J. Physics, **4**, 41, (2002); H. Kosaka *et al.*, Electron. Lett. **39**, 1199 (2003); C. Gobby, Z.L. Yuan, and A.J. Shields, Appl. Phys. Lett. **84**, 3762 (2004); X.-F Mo *et al.*, Opt. Lett. **30**, 2632 (2005); G.Wu, J. Chen, Y. Li, L.-L. Xuand H.-P. Zeng, quant-ph/0607099.

[13] B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995); H.P. Yuen, Quantum Semiclassic. Opt. **8**, 939 (1996)

[14] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000); N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44 (2002).

[15] H. Inamori, N. Lütkenhaus, D. Mayers, quant-ph/0107017; D. Gottesman, H.K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[16] Y. Zhao *et al.*, Phys. Rev. Lett. **96**, 070502 (2006); Y. Zhao *et al.*, quant-ph/0601168.

[17] C. Z. Peng et al, quant-ph/0607129.

[18] D. Rosenberg et al, quant-ph/0607186.

[19] Xiang-bin Wang, quant-ph/0609081.